RSAC 2025 Conference

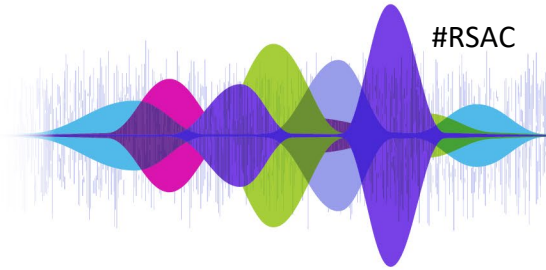
Many Voices.
One Community.

SESSION ID: PART1-T10

Ducks in a Row—How to Effectively Manage the Remediation Lifecycle

Nadir Izrael
CTO & Co-Founder
Armis
https://www.linkedin.com/in/nadiriz/

Curtis Simpson
CISO & Chief Advocacy Officer
Armis
https://www.linkedin.com/in/curtis-simpson-8156326b/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Let's Start With Some Numbers

40,187

Vulns

in 2024.
13,610 were either critical or high

3X

Exploits

increase in exploitation of vulnerabilities as an initial point of entry

137

MTTR

Days Average # of days it took for critical vulns to be addressed

60%

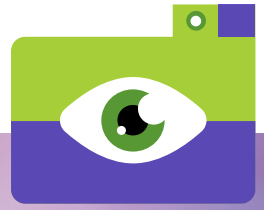
Backlog

Average number of vulns left unaddressed in an average org

Incidents Due To A Remediation Failure

Firewall Vendor

A 5 year campaign of cat and mouse between a firewall vendor and a Chinese hacking group



File Transfer Service (2023)

100 million individuals impacted despite the availability of patches

Healthcare

Remote code vuln which led to service outages of payment processing & care coordination. The vuln had a patch that was not yet applied

CPS Manufacturer

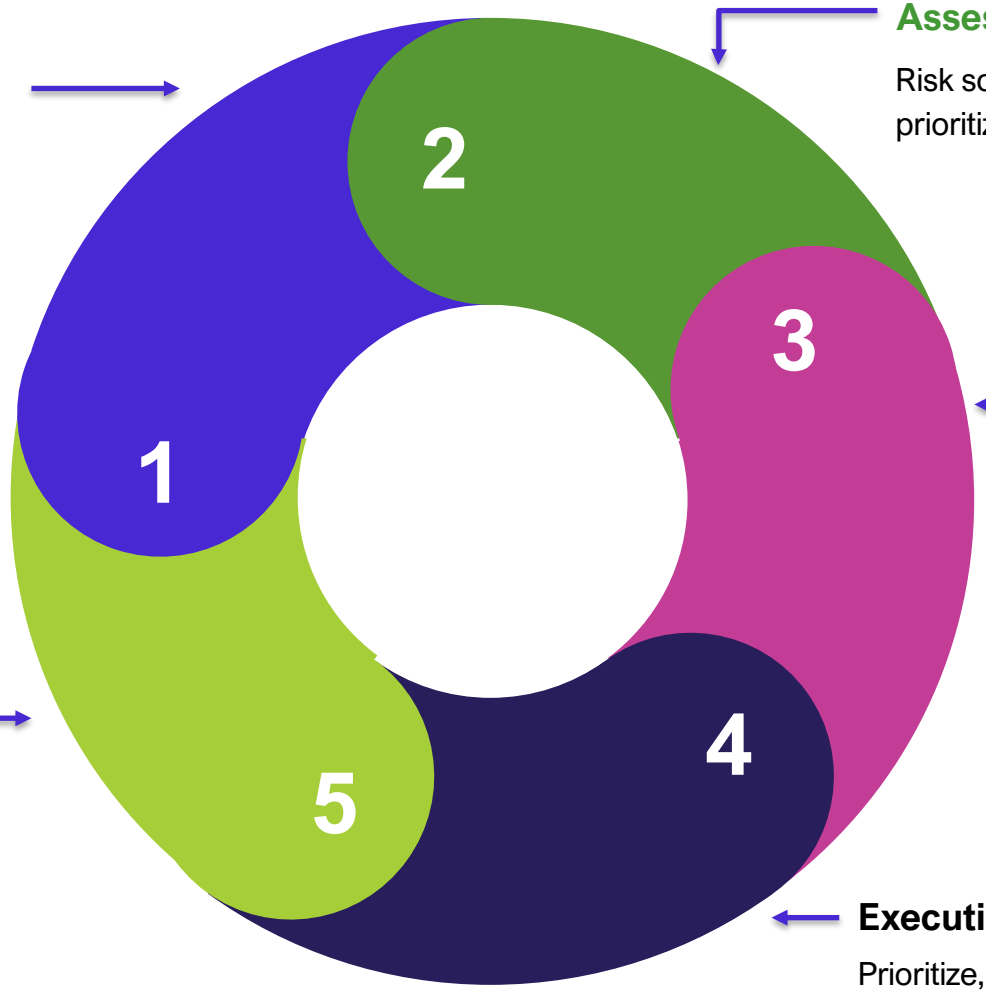
Data exfiltration and ransomware due to an unpatched vuln on a VPN

The Purpose Of This Talk

How can we effectively manage the remediation lifecycle?

What tools, tips and tricks we can leverage for the good of our orgs?

The 5 Stages of Remediation



Discovery

Identify assets, discover vulns and other security issues.

Assessment

Risk scoring & prioritization

Planning

Coordinating by deduplicating, contextualizing each threat

Execution

Prioritize, assign and mitigate

Validation

Post remediation verification

Common Pitfalls

Lack of full situational awareness across all assets

Overwhelming volume of findings

A non-collaborated response

RSAC 2025 Conference

How To Solve For These Pitfalls

Steps You Can Take Right Now

Many Voices.
One Community.

The Three Questions

- What do I **have**?
- What is **important**?
- How do I **fix it**?

ARMIS®

Step 1

What do I **have**?

Gain a consolidated view of all asset types and their behavior

- Every asset whether physical or virtual
- Integrated and collaborating with your existing security stack
- Deep situational awareness down to version numbers, backplane, accessibility, patch level, etc.

Step 2

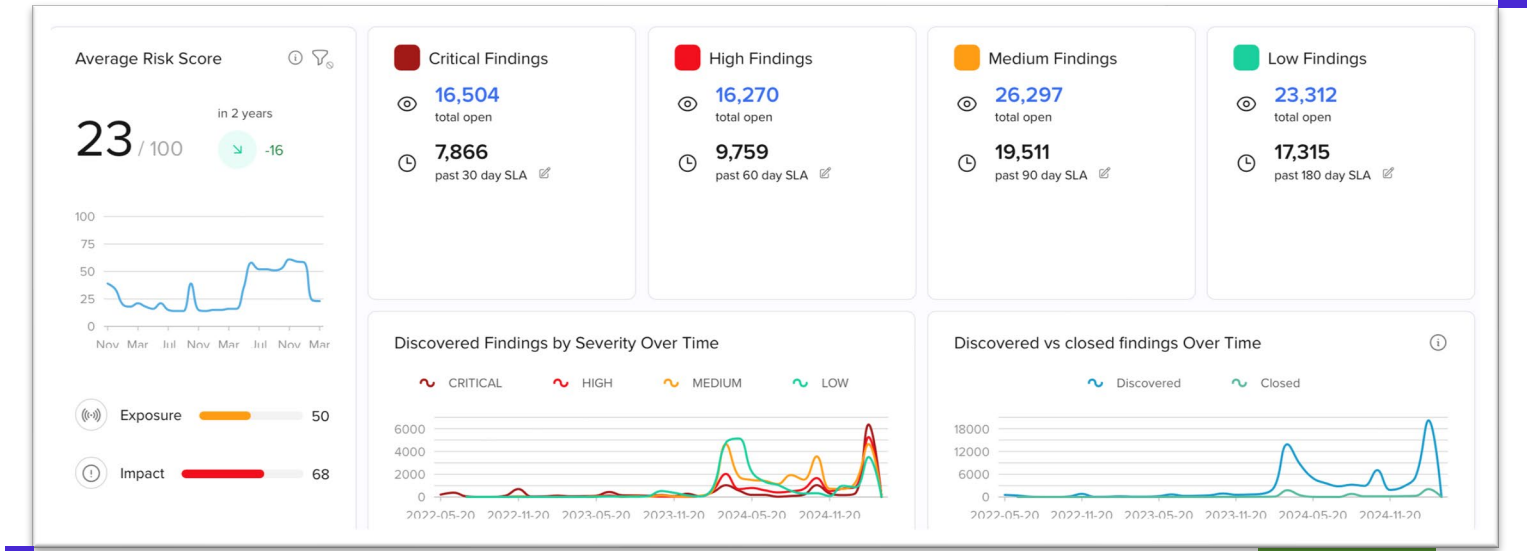
What is **important**?

Deduplicate, contextualize, prioritize findings and alerts that pose the greatest risk to your business

With Automation

80%

less time spent on manual assessment of alerts and prioritization



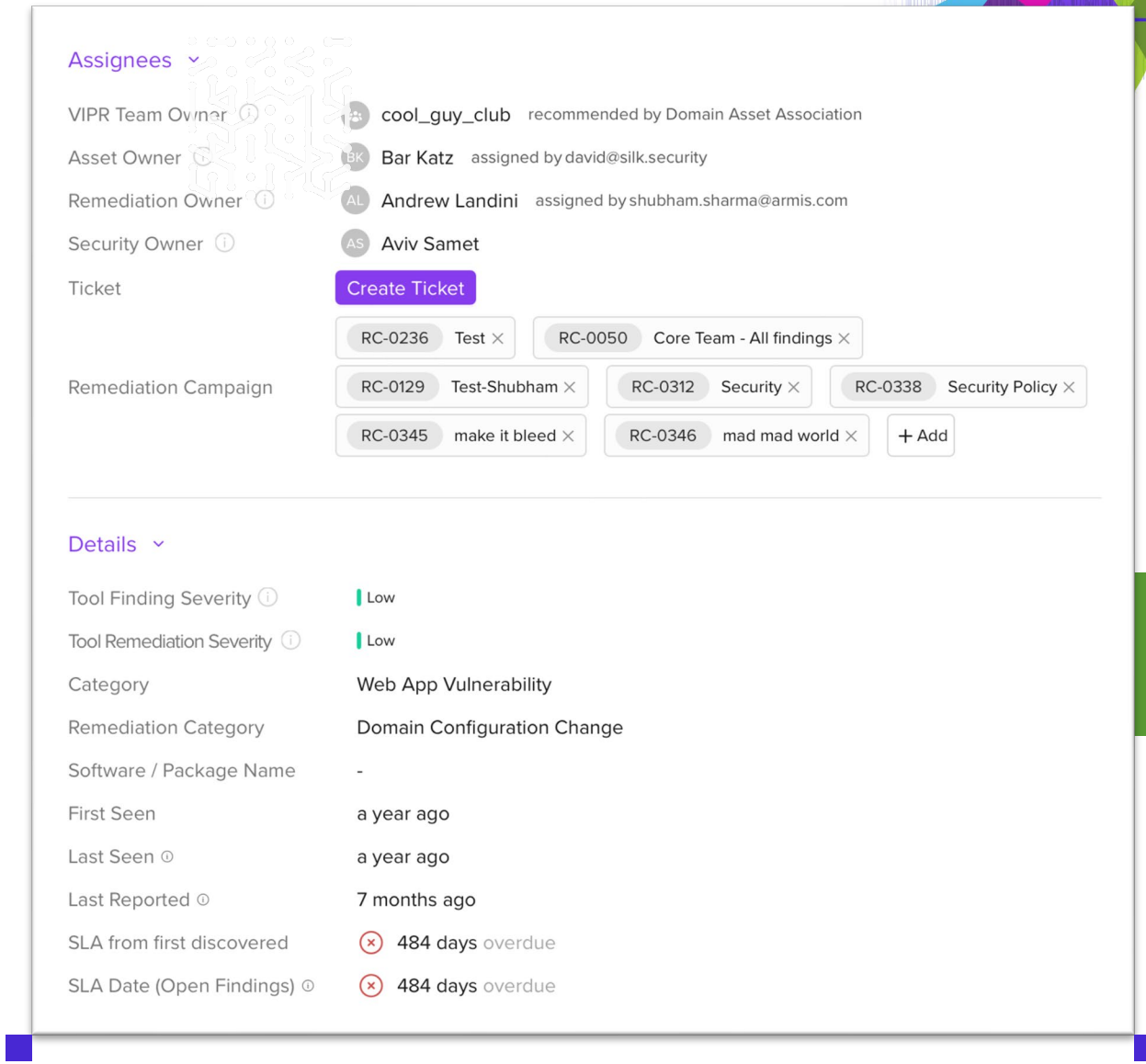
Step 3

How do I **fix it**?

Connecting the
Findings to the Fix

75%

improved MTTR for the
right findings to reduce risk



RSAC 2025 Conference

We Can Do Better!

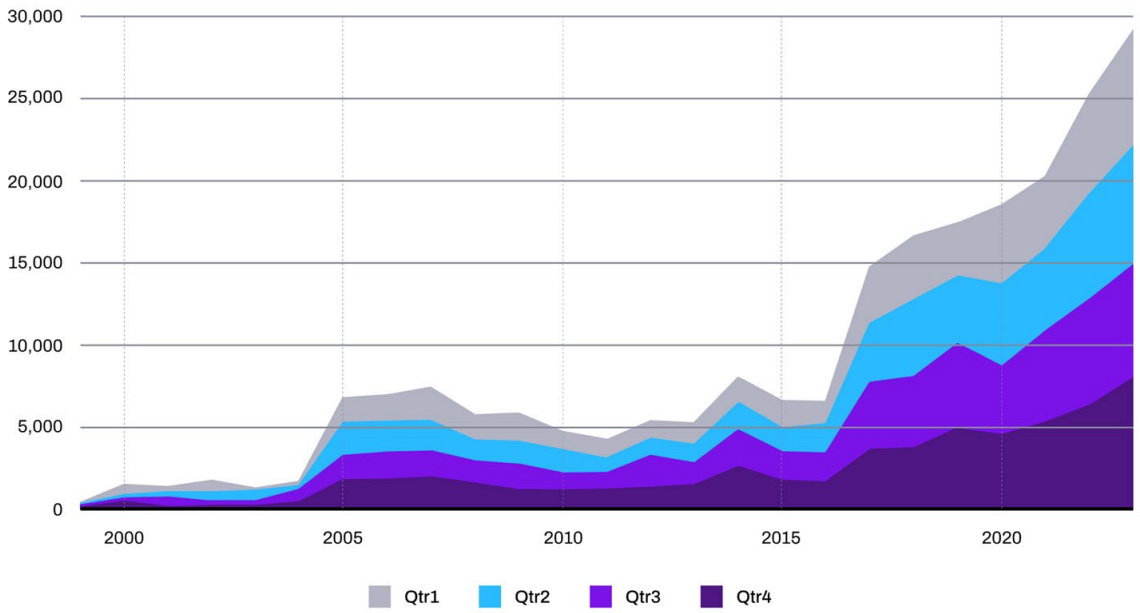
Mitigating for left of “Boom”

Many Voices.
One Community.

Legacy Vulnerability Prioritization Is Failing

The attack surface is ever-expanding and threat actors leverage AI to exploit vulnerabilities

Total CVEs Over Time



Unable to prioritize the vulnerabilities that matter most

- Operating in reactive mode with a backlog of vulnerabilities to manage.
- In the dark about what vulnerabilities to prioritize first.
- CVSS, CISA KEV, EPSS provide little guidance on the criticality of a vulnerability to your business.

© 2025 ARMIS, INC.

ARMIS

RSAC 2025 Conference

Early Warning

The Ultimate Risk Prioritization Filter

List of vulnerabilities that are being exploited in the wild or are about to be weaponized.

Proactive
Reduce vulns by addressing the most pressing first

Evidence-Based
Leverage AI to predict hacker behavior

Preemptive
Actionability before CVE is exploited

Early Warning in Practice

OBSERVE	VALIDATE	CONFIRM	ALERT
Threat actor discusses a CVE on a dark web slack channel	**AI Intelligence** Identifies threat actors, flaws in their operations and context of their discussions. **Deception Technology** leveraging dynamic honeypot detection.	**Honeypot attack hits and identifies** known and unknown exploits in the wild.	CVE added to **Early Warning list and customers alerted.**
EARLY WARNING		EXPLOITATION	

© 2025 ARMIS, INC.

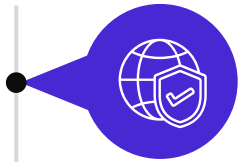
ARMIS®

RSAC 2025 Conference

Key Business Outcomes

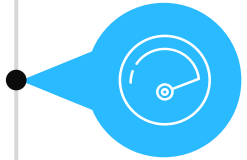
Three Goals Of This Process

Protection



Full visibility and contextualization of all assets and their behavior **reduces risk** across the environment

Time



Prioritization of findings and alerts **buy you time** to address exposures before an attack is launched

Remediation

Grouping of findings, and leveraging AI for cyber exposure management & security finds issues faster and drastically **reduces MTTR**

© 2025 ARMIS, INC.

ARMIS

RSAC 2025 Conference

Your Laundry List & Next Steps

Checklist for an Effective Remediation Lifecycle

- ✅ Complete visibility into all assets
- ✅ Risk-based prioritization beyond CVSS
- ✅ Early warning proactive threat hunting
- ✅ Automated workflows & AI-driven insights
- ✅ Security + IT collaboration frameworks
- ✅ Continuous monitoring & validation

© 2025 ARMIS, INC.

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You

Come Visit Us

Armis Booth N-5457

www.armis.com